

Single Sign On (SSO) - SAML

Introduction:

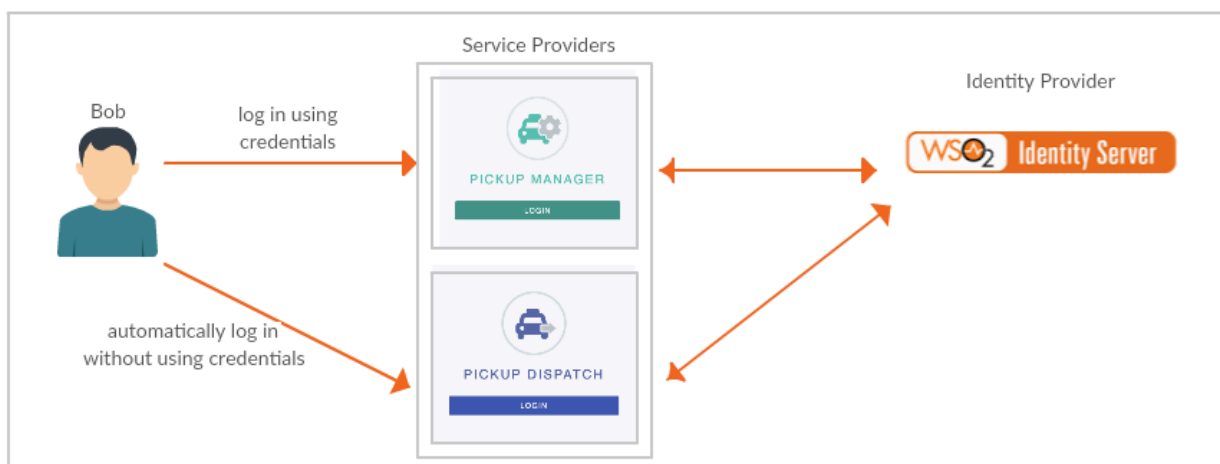
Pickup is a cab company that has many employees and different internal enterprise applications. Following are two such applications:

- **Pickup Dispatch:** This application helps manage the overall operations at Pickup.
- **Pickup Manager:** This application helps allocate vehicles to drivers.

Pickup is using **WSO2 Identity Server** as the identity provider for their applications.

Bob is a Pickup employee who usually forgets application passwords. As a result, Bob uses the same credentials for all the Pickup applications. However, due to busy schedules, Bob does not like entering the credentials at every login. So, the WSO2 Identity Server team suggested Bob to use Single Sign-On (SSO).

With SSO, Bob only needs to provide the login credentials to one Pickup application and automatically be logged in to other Pickup applications.



This tutorial will allow you to have hands-on experience on how to configure **SSO** with WSO2 Identity Server using **SAML protocol**.

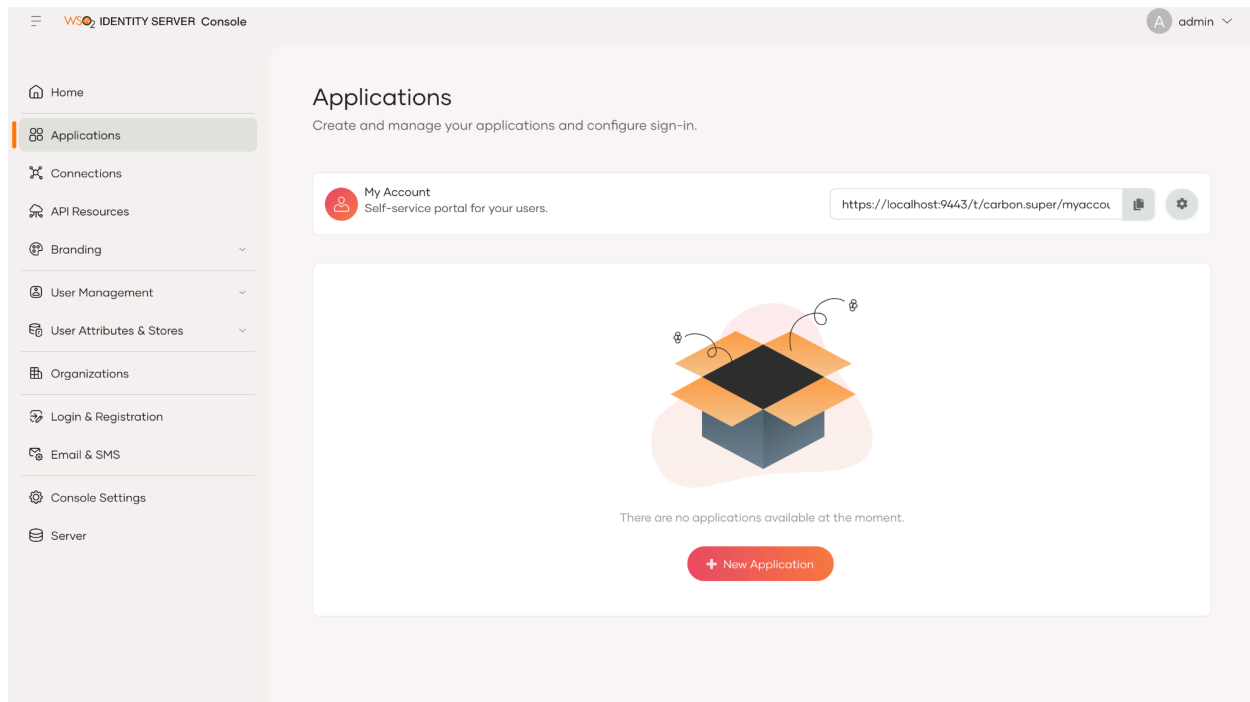
Setting up:

1. Download a tomcat server [8](#) or [9](#), run the server on port 8080.
2. Download the [saml2-web-app-pickup-dispatch.com.war](#) and [saml2-web-app-pickup-manager.com.war](#) and deploy them in tomcat.

ex: Move the `saml2-web-app-pickup-manager.com.war` to the
`<TOMACAT_PATH>/webapps`

Configure Service Providers

1. Login to the WSO2 Identity Server **Console**, using your admin credentials (ex: admin:admin).
2. In the WSO2 Identity Server **Console**, from the menu click **Applications**.



3. Click **New Application**.
4. From the given set of templates, select **Traditional Web Application** template.
5. Fill the fields in the **create application** wizard.

Name: *Pickup Dispatch*

Protocol: *SAML*

Issuer: *saml2-web-app-pickup-dispatch.com*

Assertion consumer service URLs:

http://localhost.com:8080/saml2-web-app-pickup-dispatch.com/home.jsp

Traditional Web Application
A web application that runs application logic on the server.

Dispatch

Protocol

OpenID Connect SAML

Manual File Based URL Based

Issuer *

saml2-web-app-pickup-dispatch.com

Assertion consumer service URLs *

http://localhost.com:8080/saml2-web-app-pickup-dispatch.com/hor

Cancel Create

Help

Name
A unique name to identify your application.
E.g., My App

Protocol
The access configuration protocol which will be used to log in to the application using SSO.

Issuer
The **saml:issuer** element that contains the unique identifier of the application. The value added here should be specified in the SAML authentication request sent from the client application.
E.g., my-app.com

Assertion consumer service URLs
The URLs to which the browser is redirected to upon successful authentication. Also known as the Assertion Consumer Service (ACS) URL of the service provider.

6. Click **Create**.

7. Goto the Protocols tab and click on the check box to **Enable Response Signing**.

WSO₂ IDENTITY SERVER Console

admin

Home Applications Connections API Resources Branding User Management User Attributes & Stores Organizations Login & Registration Email & SMS Console Settings Server

Response Signing

☒ Sign SAML responses

This specifies whether the SAML responses generated by WSO2 Identity Server should be signed.

Digest algorithm

http://www.w3.org/2001/04/xmldsig#sha256

Signing algorithm

http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

Single Sign-On Profile

Bindings

☒ HTTP Post

☒ HTTP Redirect

☐ Artifact

This specifies the mechanisms to transport SAML messages in communication protocols.

☐ Enable IdP initiated SSO

This specifies whether to initiate Single Sign-On (SSO) from the IdP instead of the application.

Assertion

8. Next, repeat the same steps 3-7 to create a new service provider for **pickup-manager** application. Use the below values for the required fields.

Name: *Pickup Manager*

Protocol: *SAML*

Issuer: *saml2-web-app-pickup-manager.com*

Assertion consumer service URLs:

<http://localhost.com:8080/saml2-web-app-pickup-manager.com/home.jsp>

9. Now you are ready to try out the sample with SAML SSO.
10. Restart the WSO2 Identity Server.

Try It:

1. Go to <http://localhost.com:8080/saml2-web-app-pickup-dispatch.com> and click on the login button.
2. You will be redirected to the login page of the WSO2 Identity Server. Log in using your user credentials.
3. You will be redirected to [saml2-web-app-pickup-dispatch.com](http://localhost.com:8080/saml2-web-app-pickup-dispatch.com) application home page.
4. Now if you go to <http://localhost.com:8080/saml2-web-app-pickup-manager.com>, and click the login button, you can see that the user has automatically logged in to this application.